Lobachevskii Journal of Mathematics 2013 vol.34 N4, pages 316-318

Application of composition primitive polynomials for implementation of large-scale S-boxes

Tho H.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

In this paper, the method of constructing algorithm for the implementation of large-scale S-box is proposed. Method is based on the composition primitive polynoms under GF(2) allowing to maximize the performance of S-box of a given implementation on different platforms, or to minimize the complexity of a given speed. © 2013 Pleiades Publishing, Ltd.

http://dx.doi.org/10.1134/S1995080213040136

Keywords

Cryptography, Finite Fields, S-box